REMARKS

Claims 1-17, 19-24, 26-29, 31-38 and 41-44 are rejected.

Claim Amendments

Claims 1, 9, 17, 29, 34, and 41 have been amended with clarifying amendments. These amendments are supported throughout the specification, for example on page 7, lines 20-24: "new microcode may be provided which is more tolerant of certain error events than the original drive microcode".

No new matter is added.

Claim Rejections – 35 USC § 102(b)

The Patent Office rejected claims 1-4, 6-12, 14-15, 17, 19-20, 22, 23, 27-29, 31-38, and 41-43 under 35 U.S.C. 102(b) as being anticipated by Nolet (U.S. Pat. 6,138,249). The Applicants include the following comments to clearly distinguish the claimed invention over the art cited by the Examiner, and respectfully requests a favorable reconsideration of claims 1-4, 6-12, 14-15, 17, 19-20, 22, 23, 27-29, 31-38, and 41-43.

For a claim to be anticipated, each and every non-inherent limitation must be disclosed in a single reference (MPEP 2131).

Claim 1 recites:

> "A server for improving predictive failure attributes of distributed devices, comprising:
>
> a receiver for receiving, via a network, failure analysis data from individual ones of a plurality of distributed devices; where
>
> each device of said plurality of distributed devices comprises failure analysis software comprising a **predictive failure analysis algorithm** arranged for collecting failure analysis data of said distributed device and a communications device arranged for transmitting said failure analysis data to said network;
>
> wherein said server is arranged for analyzing said failure analysis data and for

> providing in response to the analysis an updated **predictive failure analysis algorithm** to the plurality of distributed devices , wherein each of said plurality of distributed devices is coupled to said network, wherein the **updated predictive failure analysis algorithm** is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein execution of the first microcode results in the updated predictive failure analysis algorithm **using different tolerances** of certain error events when **estimating an impending failure**" (emphasis added).

The Examiner states Nolet teaches:

> "a server for improving predictive failure attributes of distributed devices (column 7, lines 55-58; column 8, line 57), comprising: a receiver for receiving, via a network, failure analysis data from individual ones of a plurality of distributed devices (column 7, lines 55-60); where each device of said plurality of distributed devices comprises failure analysis software comprising a predictive failure analysis algorithm arranged for collecting failure analysis data of said distributed device (column 8, lines 29-48, wherein each device has a software agent that tests/monitors the device and transmits that information; column 1, lines 62 – column 2, line 8, wherein, the collected data at the distributed devices can be used for predicting future problems in the manufacturing process); and a communications device and [sic] arranged for transmitting said failure analysis data to said network (column 5, lines 18-29; column 8, lines 33-36; column 6, lines 48-67); wherein said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated predictive failure analysis algorithm to the plurality of distributed devices, wherein each of said plurality of distributed devices is coupled to said network, wherein the updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein the first microcode and the second microcode have different tolerances of certain error events (column 8, lines 57-59, 40-48; column 18, lines 1-4, wherein the central monitoring center gets the service requests from the devices and analyses the data to see which monitoring/testing software the device is currently running, if the currently used software is not the most up to date, the center transmits the most current updated software to the devices for the future monitoring of the devices; column 13, line 59 – column 14, line 9)" (page 2 and 3 of the Office Action dated August 28, 2007).

The Applicants respectfully assert the Examiner has misinterpreted the teachings in Nolet. The disclosure in Nolet is addressed to collecting information regarding failures: for example, when "a

failure occurs during the test process, it is desirable to maintain a record of how the failure was dispositioned" (see column 1, line 62); "if a **system fails** in the field" (see column 1, line 67 to column 2, line 1); "determine when any of the data processing systems **experiences a failure**" (column 5, lines 20-21); "indicates the **nature of the failure**" (column 7, lines 19-20); etc. (Emphasis added throughout).

In contrast, the Applicants' invention is directed at least in part to a "predictive failure analysis algorithm" which estimates "an impending failure" as in claim 1.

As Nolet is directed towards collecting information regarding a system that has failed, Nolet does not describe an ability to predict a failure. There is no mention in Nolet of predicting an "impending failure" as in claim 1. A word search of Nolet returns no results for "predict", "predictive", "statistic", "warn" or "anticipate".

The Examiner asserts "the collected data at the distributed devices can be used for predicting future problems in the manufacturing process" (page 2) and relies upon column 1, lines 62 – column 2, line 8 as supporting this statement. This section states:

> "When a failure occurs during the test process, it is desirable to maintain a record of how the failure was dispositioned. This can be particularly important in the event that a system fails in the field. One goal of the manufacture/test process is to **ensure that all errors are detected <u>before the system is shipped</u> to the customer**. Thus, if a system fails in the field, it is desirable to determine why the testing process did not detect the error prior to shipping, and to **adapt the process so that it can detect similar failures in the future**. The maintenance of records indicating the manner in which all errors on a particular system were dispositioned can be extremely **helpful in determining why a particular failure in the field was not detected** during the manufacture/test process" (emphasis added).

The Applicants assert that the Examiner has misinterpreted this section. The collected data is not used to "predict future problems", but rather "in determining why a particular failure in the field was not detected". Thus the information is not used for any prediction, but rather to "adapt the process so that it can detect similar failures in the future". It should be noted that this section places emphasis on detecting failures "before the system is shipped". Even if this section disclosed the functionality described by the Examiner, which the Applicants do not assert it does, "predicting future problems in the manufacturing process" does not disclose or suggest a "predictive failure analysis algorithms" as in claim 1.

In the Response to Arguments section the Examiner reiterates "that Nolet does teach wherein the collected data is used in future manufacturing processes to *adapt the process so that it can detect similar failures in the future*" (page 16, emphasis in the original). The Applicants assert that detecting a failure is not analogous to "estimating an impending failure" as in claim 1.

Additionally, the Examiner asserts that Nolet teaches "receiving, via a network, failure analysis data". The Applicants assert that the disclosure of Nolet does not suggest or disclose such an element. The system of Nolet is described as "when a failing one of the plurality of data processing systems experiences a failure, **storing information** in the failing one of the plurality of data processing systems **identifying a nature of the failure**, and **broadcasting a service request** from the failing one of the plurality of data processing systems to the monitoring system, the service request indicating that the failure has occurred" (col. 6, lines 57-64, emphasis added). Clearly, Nolet describes storing information "identifying a nature of the failure" and separately "broadcasting a service request" "indicating that the failure has occurred". Thus, Nolet does not disclose or suggest "receiving, via a network, failure analysis data" as in claim 1.

The Examiner asserts that Nolet discloses:

> "the central monitoring center gets the service requests from the devices and analyses the data to see which monitoring/testing software the device is currently running, if the currently used software is not the most up to date, the center transmits the most current updated software to the devices for the future monitoring of the devices".

The Examiner cities column 8, lines 57-59, 40-48; column 18, lines 1-4; and column 13, line 59 – column 14, line 9 in support. The Applicants respectfully assert this is a misinterpretation of the disclosure in Nolet.

At column 8, lines 29-64

> "To address the concern regarding inventory transactions or test file updates being missed as a result of the polling loop time … the embodiment … employs a transaction-based procedure. In particular, each of the systems 21, 23 being monitored detects situations wherein information should be **updated in the APC monitor** 25, and notifies the monitor 25. This is similar to the call home feature discussed above, except that the notification is transmitted over the network 27, rather than a modem/telephone line connection. Each of the monitored systems 21, 23 has an associated agent 29, 31. Each agent 29, 31 monitors the relevant files of its associated system 21, 23, and when any of those files is updated, the agent performs two functions. First, the **agent broadcasts a service request** to the APC monitor 25 over the network 27, indicating that there has been a change of a relevant file that the APC monitor 25 should be aware of. Second, the agent stores or queues the updated information so that as the monitored system continues to operate, the queued information will not be lost if the relevant file is updated again, and **will be available to the APC monitor** 25 when it services the request. The queuing of the information by the agent ensures that no relevant information will be lost, even if there is a delay (e.g., due to the network 27 going down) in the APC monitor 25 servicing the broadcast request. The transaction based procedure is also advantageous in that it results in real time updates of the information in the APC monitor 25.
>
> "The APC monitor 25 includes at least one server 33 that is responsible for servicing the requests broadcast by the agents 29, 31 over the network 27. In a manner that is discussed in more detail below, the servers 33 handle the broadcast requests by reading the relevant information from the requesting agent 29, 31 over the network 27, and then **updating the database** 35 with the new information provided by the agent" (emphasis added).

This database is described more fully at column 8, lines 10-15:

> "the database used during the manufacture/test monitoring process is also **used to manage the inventory** of the parts and subcomponents (collectively "parts") used in the systems under test. The database is automatically updated to **maintain accurate information** regarding the parts in each system under test" (emphasis added).

This section describes the agent providing update information to the monitor. Specifically this procedure is used to address "loss of some test data due to the polling delay" (see column 8, lines 16-17). The 'update' is actually used to provide inventory data (such as which devices have failed), not microcode. Additionally, the database being updated is used to "maintain accurate information". There is no disclosure or suggestion of the server being "arranged for analyzing" this data, such as seen in Claim 1.

Clearly, these sections, as relied upon by the Examiner, do not disclose a server where:

> "said server is arranged for analyzing said failure analysis data and for providing in response to the analysis an updated predictive failure analysis algorithm to the plurality of distributed devices, wherein each of said plurality of distributed devices is coupled to said network, wherein the updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode that is provided from the server to be used instead of a second microcode previously used by the plurality of distributed devices, wherein execution of the first microcode results in the updated predictive failure analysis algorithm using different tolerances of certain error events when estimating an impending failure" (Claim 1, emphasis added).

As was noted above, Nolet is devoid of any express reference to "predict", "predictive", "statistic", "warn" or "anticipate". Therefore, Nolet is devoid of a "predictive failure analysis algorithm" as in Claim 1. As Nolet does not disclose each and every non-inherent limitation of Claim 1, Nolet cannot anticipate Claim 1. Thus, Claim 1 is in a condition for allowance.

Furthermore, Nolet teaches that an agent is provided "a default set of files to monitor, but this list can be altered by the APC monitor" (col 12. lines 10-12) and that "the agent broadcasts a service request to determine whether any updates should be made to its **list of files to be monitored**" (col. 12, lines 23-25, emphasis added). Clearly there is **no indication that the "list of files to be monitored" of Nolet is executable**. Thus the "list of files to be monitored" of Nolet is not analogous to the "microcode" of claim 1. Therefore, Nolet does not disclose or suggest an "updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode" or "execution of the first microcode results in the updated predictive failure analysis algorithm using different tolerances of certain error events when estimating an impending failure" as in claim 1.

Independent claims 9, 17, 29, 34, and 41 share many similarities with claim 1; therefore, many of the above arguments apply to these claims as well.

Claim 9 recites:

> "A device comprising:
>
> a **predictive failure analysis algorithm** arranged for collecting failure analysis data of said device; and,
>
> a communications device coupled to said predictive failure analysis algorithm arranged for **transmitting said failure analysis data** to a remote server via a network,
>
> wherein said remote server is **arranged for analyzing said failure analysis data** received from said device and from other devices and for **providing an updated predictive failure analysis algorithm** to the device and the other devices, wherein the updated predictive failure analysis algorithm is provided to the device in the form of a first microcode that is provided from the remote server to be used instead of a second microcode previously used by the device and the other devices, wherein execution of the first microcode results in the updated predictive failure analysis algorithm **using different tolerances** of certain error events when **estimating an impending failure**" (emphasis added).

Claim 17 recites:

> "A method for performing predictive data analysis using a central server, said method comprising:
>
> collecting failure analysis data in individual ones of a plurality of distributed devices in which **each of the distributed devices uses a predictive failure analysis algorithm**;
>
> receiving said failure analysis data at the central server from a network coupled to each device of said plurality of distributed devices; **analyzing said failure analysis data** received from said each device at the central server; and
>
> **in response to the analysis, providing an updated predictive failure analysis algorithm** from the central server to the distributed devices, wherein the updated predictive failure analysis algorithm is provided to the plurality of distributed devices in the form of a first microcode that is provided from the central server to the plurality of devices to be used instead of a second microcode previously used by the plurality of devices, wherein execution of the first microcode results in the updated predictive failure analysis algorithm **using different tolerances** of certain error events when **estimating an impending failure**" (emphasis added).

Claim 29 recites:

> "A computer program comprising computer readable program code stored on a computer readable medium for performing failure analysis of a plurality of disk drives that comprise a part of at least one data storage system, comprising first program code for collecting failure analysis data from individual ones of said disk drives and for transmitting said collected failure analysis data to a central server via a network and second program code, executed at said central server, for analyzing said failure analysis data and **deriving an updated predictive failure analysis algorithm** therefrom, where **said updated predictive failure analysis algorithm is downloaded** to said plurality of disk drives via the network, wherein the updated predictive failure analysis algorithm is provided to the plurality of disk drives in the form of a first microcode from the central server to be used instead of a second microcode previously used by the plurality of disk drives, wherein execution of the first microcode results in the updated predictive failure analysis algorithm **using different tolerances** of certain error events when **estimating an impending failure**" (emphasis added).

Claim 34 recites:

> "A computer program comprising computer readable program code stored on a computer readable medium for performing failure analysis of a plurality of disk drives that comprise a part of at least one data storage system, comprising first program code, executed by a central server, for receiving, via a network , failure analysis data from said at least one data storage system for analyzing said failure analysis data and for **deriving an updated predictive failure analysis algorithm** therefrom, where **said updated predictive failure analysis algorithm is downloaded** to said plurality of disk drives via said network, wherein the updated predictive failure analysis algorithm is provided to the plurality of disk drives in the form of a first microcode to be used instead of a second microcode previously used by the plurality of disk drives, wherein execution of the first microcode results in the updated predictive failure analysis algorithm **using different tolerances** of certain error events when **estimating an impending failure**" (emphasis added).

Claim 41 recites:

> "A system for monitoring performance of a plurality of distributed devices via a network, comprising:
>
> a network;
>
> a central server having a monitoring capability, the central server being coupled to the network;
>
> a plurality of distributed devices which are coupled to the network and which are monitored by the central server via the network, each of the plurality of distributed devices having a failure data analysis capability **provided by a predictive**

> **failure analysis algorithm** of the corresponding distributed device, each of the plurality of distributed devices providing predictive failure data to the central server via the network, wherein the **central server modifies the predictive failure analysis algorithm** in the form of a first microcode based on the predictive failure data to provide an updated predictive failure analysis algorithm in the form of a second microcode previously used by the plurality of distributed devices, wherein execution of the first microcode results in the updated predictive failure analysis algorithm **using different tolerances** of certain error events when **estimating an impending failure**" (emphasis added).

Thus, Nolet does not anticipate independent claims 1, 9, 17, 29, 34, and 41. Claims 2-4, 6-8, 10-12, 14-15, 19-20, 22, 23, 27-28, 31-33, 35-38, and 42-43 are dependent claims and are allowable because their corresponding base claims are allowable.

In light of the discussion above, the Applicants respectfully assert that a case for anticipation was not presented. As such, the Applicants respectfully request that the Examiner reconsider and withdraw these rejections.

Claim Rejections – 35 USC § 103(a)

The Examiner has rejected claims 5, 13, 16, 21, 24, 26 and 44 as being unpatentable under 35 U.S.C. 103(a) over Nolet in view of Ballard (U.S. Publ. Pat. No. 2003/0088538). The Applicants include the following comments to clearly distinguish the claimed invention over the art cited by the Examiner, and respectfully request a favorable reconsideration of claims 5, 13, 16, 21, 24, 26 and 44.

The Examiner refers to a reference "Ballrd" (page 12). It is assumed the Examiner intended to refer to Ballard (U.S. Publ. Pat. No. 2003/0088538), but if this not the case, the Applicants request the Examiner to provide detailed information regarding this reference.

It is well established law that in order for an obviousness rejection to be proper, the Patent Office must meet the burden of establishing a prima facie case for obviousness. Thus, as interpreted by the Courts, the Patent Office must meet the burden of establishing that all elements of the invention are disclosed in the prior art and that in accordance with *In re Lee*, the prior art must contain a suggestion, teaching, or motivation for one of ordinary skill in the art to modify a reference or combine references; and that the proposed modification must have had a reasonable expectation of success, determined from the vantage point of the skilled artisan at the time the invention was made.[1]

As noted above, Nolet does not disclose or suggest the independent claims. Ballard is not presented as remedying the deficiencies of Nolet. As neither Nolet nor Ballard disclose a "predictive failure analysis algorithm", the combination does not teach this element as well. Therefore, for at least this reason the combination of Nolet and Ballard does not make obvious the independent claims 1, 9, 17, 29, 34, and 41.

Claims 5, 13, 16, 21, 24, 26 and 44 are dependent upon claim 1, 9, 17, or 41 and are allowable because their corresponding base claims are allowable.

In light of the discussion above, the Applicants respectfully assert that a prima facie case for obviousness was not presented as required by the court in *In re Lee*. As such, the Applicants respectfully request that the Examiner reconsider and withdraw these rejections.

For the foregoing reasons, the Applicants believe that each and every issue raised by the Examiner has been adequately addressed and that this application has now been placed in a condition for allowance. As such, early and favorable action is respectfully solicited.

[1] *In Re Fine5 U.S.Q.2d 1596, 1598 (Fed. Cir. 1988); In Re Wilson, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970); Agmen v. Chugai Pharmaceuticals Co., 927 U.S.P.Q.2d, 1016, 1023 (Fed. Cir. 1996); In Re Sang Su Lee, 277 F.3d 1338, 61 U.S.P.Q.2d 1430 (Fed. Cir. 2002).*

Respectfully submitted:

Harry Smith

10/30/2007

Harry F. Smith

Date

Reg. No.: 32,493

Customer No.: **49132**

HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203) 925-9400
Facsimile: (203) 944-0245
email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

Date

Name of Person Making Deposit